

The Honorable John C. Coughenour

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA,

Plaintiff,

v.

RYAN S. HERNANDEZ,

Defendant.

NO. CR19-259JCC

**UNITED STATES' SENTENCING
MEMORANDUM**

Sentencing Date: December 1, 2020

The United States of America, by and through undersigned counsel, files this Memorandum in anticipation of the sentencing hearing in the aforementioned matter. Sentencing is scheduled for December 1, 2020, to be held by videoconference.

I. INTRODUCTION

The defendant, Ryan S. Hernandez, comes before the Court for sentencing on his guilty pleas to two felony counts: *Computer Fraud and Abuse*, in violation of Title 18, United States Code, Section 1030(a)(2), and *Possession of Child Pornography*, in violation of Title 18, United States Code, Section 2252(a)(4)(B). For the reasons set forth below, and as set forth in the parties' Plea Agreement, the United States respectfully recommends that the Court impose sentences of **36 months** on each count, to run concurrently, to be followed by seven (7) years of supervised release. The U.S. Probation Office and Defendant

Hernandez also jointly recommend a custodial sentence of 36 months.

As discussed below, despite repeated warnings, Defendant Hernandez has tormented Nintendo for years by stealing and exposing confidential and proprietary information about the company's various games and consoles. Most recently, he hacked multiple server groups to access developer tools and internal files and data relating to, among other things, pre-release video games and game consoles. As also uncovered through this investigation, Defendant Hernandez had stockpiled over 1,600 total images and videos of minors engaged in sexually explicit conduct, which he stored electronically on his digital devices in his residence.

In short, a custodial sentence of some significance is warranted. The United States submits that the jointly recommended sentence adequately accounts for the various sentencing factors and is appropriate under the totality of the circumstances.

II. BACKGROUND

A. Offense and Relevant Conduct

The Presentence Report ("PSR") prepared by the United States Probation Office, dated November 3, 2020, and the parties' Plea Agreement (Dkt. #11), provide an accurate overview of the offense conduct of the defendant, Ryan Hernandez.

1. Computer Hacking Activity and Theft of Proprietary Information

As discussed below, Defendant Hernandez, who also uses the alias "Ryan West" and the online moniker "RyanRocks," has an extensive history of targeting and exploiting Nintendo and its products.¹ Through multiple separate endeavors over the course of years, which has continued nearly unabated through June 2019, when FBI agents searched his residence and seized his electronic devices, Hernandez hacked into protected computers of Nintendo and stole or misused non-public and proprietary data, most commonly related to

¹ Nintendo is a consumer electronics and video game company. Nintendo Co., Ltd, is headquartered in Japan, and its North American subsidiary, Nintendo of America, is located in Redmond, Washington. Nintendo has manufactured a variety of home and handheld game consoles, such as the Wii U, 3DS, and the Switch, and developed multiple popular video game franchises, such as Mario, The Legend of Zelda, Pokémon, Animal Crossing, and Splatoon, among others.

1 developer tools, pre-release video games, and game consoles. Hernandez shared such
 2 information with others through various social media and online portals. Despite prior
 3 contacts by Nintendo representatives and law enforcement, Hernandez persisted relentlessly
 4 in such conduct.

5 ***a. 2016 Abuse of Nintendo Developer Portal and Dissemination of***
 6 ***Confidential Information***

7 In 2016, Hernandez registered for Nintendo developer access, which, among other
 8 things, required that he accept the terms of a non-disclosure agreement governing the use
 9 and disclosure of information. The Developer Portal is an online resource intended for
 10 individuals' legitimate use in developing video games and video game consoles.

11 Without authorization from Nintendo, Hernandez accessed confidential and
 12 proprietary information, including material for the Wii U console and Nintendo 3DS
 13 system, through Nintendo's online developer sites. In violation of the terms of the non-
 14 disclosure agreement and various laws, he publicly posted and disclosed such information.
 15 Such disclosures of confidential and proprietary information increased the risk of piracy of
 16 Nintendo products, among other harms caused to Nintendo.

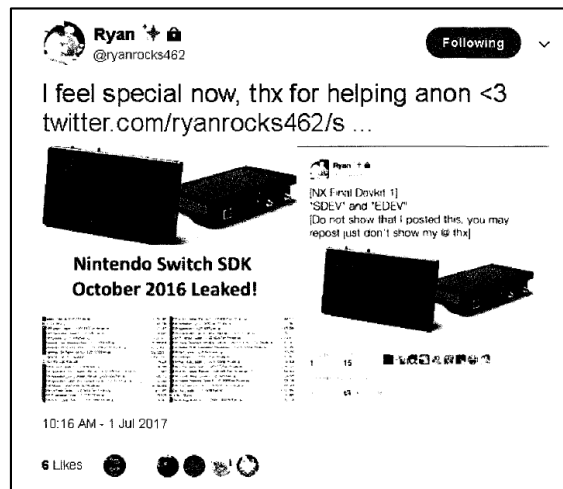
17 Nintendo, through its representatives, contacted Hernandez demanding he cease and
 18 desist such conduct. On September 30, 2016, Hernandez, then a minor, and his parents
 19 agreed that Hernandez would discontinue such conduct and cease use of Nintendo's
 20 developer sites and confidential and proprietary information.

21 ***b. 2016 Hack of Nintendo Developer Portal and Dissemination of***
 22 ***Confidential Information***

23 In October 2016 (*i.e.*, within a month of the above-mentioned agreement with
 24 Nintendo), Hernandez assisted an associate compromise Nintendo's online Developer
 25 Portal, described above. Hernandez sent a phishing message under a fake name, falsely
 26 requesting technical support, posted to a Nintendo online forum to trick a Nintendo
 27 employee to click on an external link embedded in the message. As designed, the link
 28 directing the Nintendo employee to an external site hosting a malware program that secretly

scraped the employee's information and authentication tokens. Hernandez's associate then used the employee's stolen tokens to upload malware onto the Nintendo developer site, which logged the tokens of legitimate users logging onto the site, and later to gain administrator access to the Developer Portal. The associate then used the stolen user tokens to download proprietary Nintendo data.

Some of the stolen data, including pre-release information about the highly anticipated Nintendo Switch console, was leaked to the public on various forums as early as October 2016, months before its official release,² which caused Nintendo substantial monetary harm. In July 2017, Hernandez, using Twitter account @ryanrocks462, publicly took credit for participating in the leak of data related to the Nintendo Switch SDK:



On October 25, 2017, FBI agents contacted Hernandez at his residence in Palmdale, California. During that consensual interview, conducted in the presence of his parents, Hernandez admitted his role in the hack of the Developer Portal. He promised to stop any further malicious activity against Nintendo and confirmed his understanding of the potential consequences of hacking conduct.³ Hernandez was not arrested or charged in relation to that illegal activity. Once again, Hernandez's promises proved empty.

² The Nintendo Switch console was officially released in March 2017.

³ During the interview, Hernandez responded to agents' questions predominantly in writing and through gestures.

1 ***c. 2018-2019 Hack of Nintendo Servers and Dissemination of***
 2 ***Proprietary Information***

3 Despite his assurances to Nintendo and FBI agents, Hernandez continued to
 4 victimize Nintendo and thereafter hacked into various servers belonging to Nintendo,
 5 similarly targeting information about developer tools, video games, and consoles, including
 6 products still under development and others not yet released publicly.

7 Beginning in or before June 2018, and continuing until June 2019 (when agents
 8 again contacted him and searched his residence), Hernandez accessed, without
 9 authorization, various Nintendo server groups and downloaded confidential and proprietary
 10 information. For example, one of the server groups targeted by Hernandez related to a
 11 staging environment for the Nintendo eShop, which is used for pre-production testing. In
 12 June 2018, Hernandez accessed the servers, using without authorization a legitimate
 13 certificate, and requested and downloaded pre-release information and data, including
 14 development tools and files relating to retail titles.

15 Similarly, beginning later in June 2018, Hernandez accessed the device
 16 authentication server group using an illegitimate certificate obtained from an application
 17 extracted from the previously compromised staging environment server group, described
 18 above.

19 Beginning in July 2018, Hernandez accessed the server group that managed content
 20 for Nintendo retail kiosks, including advertising material and game demos. Hernandez's
 21 conduct continued on in this fashion through 2018 and into 2019.

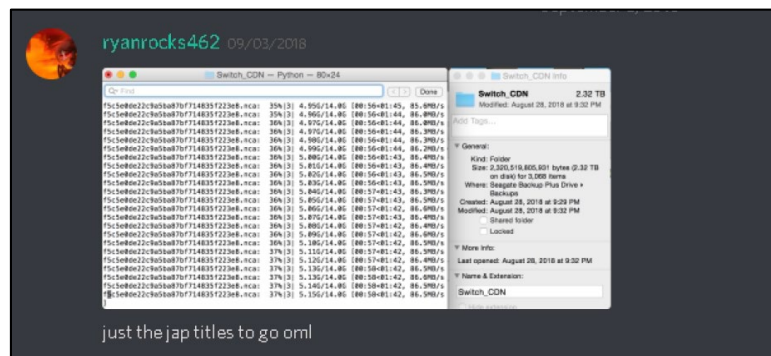
22 The servers compromised by Hernandez were located in various states, including
 23 Washington (within this District) and Oregon, and in some cases abroad, and were used in
 24 and affect interstate and foreign commerce and communication.

25 ***d. Hernandez's Distribution and Use of Stolen Victim Data***

26 Hernandez posted extensively about his hacking exploits and leaked stolen
 27 information using various online platforms, such as Twitter and Discord.
 28

In fact, Hernandez operated an online forum on Discord⁴ specifically dedicated to Nintendo and Nintendo products called “Ryan’s Underground Hangout.” Through this Discord forum, which enables users to create chatrooms (called “servers”) where participants can communicate through posts and/or direct messages as well as through voice or video chat, Hernandez and his associates collaborated regarding possible system vulnerabilities. Hernandez also shared details of downloaded content and information about compromised Nintendo servers and file directories. Below are a few illustrative examples of Hernandez’s conduct over Discord:

- Hernandez (Discord user “ryanrocks462”) claimed to have access to Nintendo servers and was actively downloading content, specifically related to the Nintendo Switch. On August 28, 2018, Hernandez posted a screenshot of what appeared to be a file folder titled “Switch_CDN”⁵ along with the message: “2 more Terabytes and ill have all of nintendos cdn.” On about September 3, 2018, Hernandez posted a similar image of the “Switch_CDN” file folder with the message: “just the jap titles to go oml”:⁶

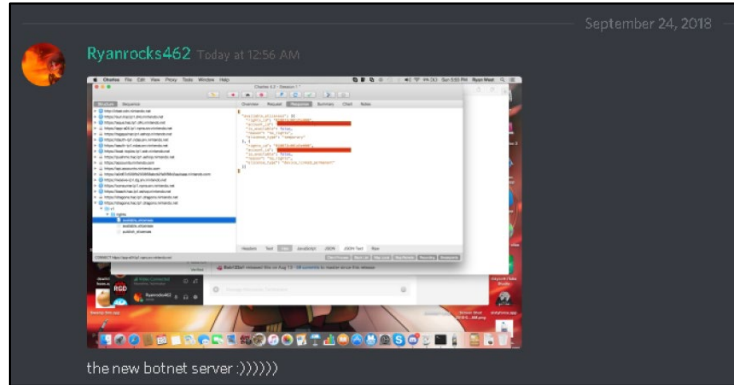


- On September 24, 2018, Hernandez posted an image showing what appears to be domains, along with the message: “the new botnet server :))))))”:

⁴ Discord is an online communication platform that offers users voice and video call, messaging, chatroom, and file-sharing services.

⁵ A Content Delivery Network, or “CDN,” refers to a method by which data is transmitted by using a system of distributed servers that deliver the content based on your geographic location. This helps speed up data transfer.

⁶ According to various online reference sites, “oml” typically means “Oh My Lord” in Internet slang. The term “jap” is a slang, often derogatory, term for Japanese. Nintendo Co., Ltd, is a Japanese company and markets games to numerous markets worldwide, including in Japan.

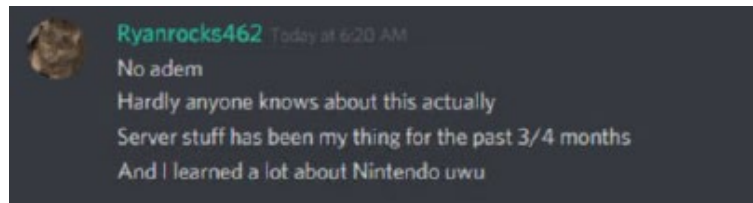


In this message, Hernandez displayed external computers under his remote unauthorized control.

- On October 17, 2018, Hernandez posted a screenshot and stated that others were allowed to use his Amazon server as a LAN host,⁷ which appeared to allow users to access pirated Nintendo games and products.

- On December 16, 2018, Hernandez posted an image of the file directory on fileshare.nintendo-europe.com and commented that files related to the Switch console had been added.

- On February 4, 2019, Hernandez indicated that he needed to test a new piracy patch and posted multiple screenshots that he described as Nintendo internal servers. He further indicated that these images included Nintendo's internal eShop API testing server (which, as discussed above, is one of the server groups Hernandez hacked). Hernandez further indicated that he had been working on Nintendo "Server stuff" for the past 3 to 4 months and had learned a lot about Nintendo:



⁷ A Local Area Network, or "LAN," typically refers to a group of interconnected computers.

1 In Discord communications, Hernandez also referenced his involvement in the prior
 2 hack of Nintendo's Developer Portal. For example, on November 24, 2018, Hernandez
 3 commented about how the FBI had previously come to his residence regarding his hack of
 4 Nintendo. Hernandez added that, if the FBI visited again, he would tell the FBI "you will
 5 lose the case just [like] last time !" Further, on December 22, 2018, Hernandez asked others
 6 for available storage, either on their computer or on a Google Drive, indicating he need
 7 "like 400GB" for a backup that possibly included "30,000 + links" and "pre-release stuff
 8 to." Hernandez also suggested that the files related to "3ds/wiiu probably." Hernandez then
 9 told another Discord user "U have to phish SDSG[,] Like anon did for me with the 16.7
 10 sdk" and further explained the phishing methodology.⁸

11 *e. Search of Hernandez's Residence and Seizure of Devices*

12 On June 19, 2019, FBI agents conducted a warrant search on Hernandez's residence
 13 in Palmdale, California. Therein, they recovered various electronic devices from
 14 Hernandez's bedroom, including a Seagate external hard drive containing thousands of
 15 confidential Nintendo files related to video games, consoles, and developer tools, and
 16 multiple devices used to facilitate the unauthorized access of Nintendo servers.
 17 Investigators also recovered several circumvention devices used to access pirated games and
 18 other proprietary content.

19 **2. Possession of Child Pornography**

20 For some period of time, continuing up through June 19, 2019, when FBI agents'
 21 search his residence and seized his various electronic devices, Defendant Hernandez also
 22 knowingly possessed visual depictions of minors engaged in sexually explicit conduct (child
 23 pornography), which he stored electronically on his digital devices. For instance, on the
 24 aforementioned Seagate external hard drive recovered from his bedroom, Hernandez
 25 possessed approximately 669 graphics and 968 videos of actual minors, including
 26
 27

28 ⁸ To be clear, investigators believe Hernandez was the one providing assistance to an associate who was the primary actor in conducting the 2016 hack of the Developer Portal.

1 prepubescent minors, engaged in sexually explicit conduct, which he downloaded from the
2 Internet.

3 The child pornography files were stored in a folder directory called “Bad Stuff,”
4 further organized within subfolders that appear to reflect a rating system based on personal
5 preference (titled “cute,” “eh,” “okish,” etc.).

6 Three of the 968 illicit videos are described below:

- 7 • File 1: “BR160 12 and 7 Year Old Cousins Suck Fuck 69 And Jerk + Get
8 Caught.avi”

9 This 50-minute video depicts two prepubescent males on a webcam sitting on
10 what appears to be a bed. Both males remove their clothing and proceed to
11 engage in both manual and oral sex. Based on lack of pubic hair, muscular
12 development, and youthful appearance, both males are approximately between 7
and 12 years old (as indicated by the file name).

- 13 • File 2: “2 boys hard fuck xxx.avi”

14 This 20-minute video depicts a naked prepubescent male laying on a bed. A
15 second prepubescent male is shown removing his clothing and joining the first
16 male on the bed. The video continues to show the pair engaging in oral and anal
17 sex. Based on lack of pubic hair, muscular development, and youthful
appearance, both males are approximately 12 years old.

- 18 • File 3: “9 Year Old Zachary And Kevin Suck Jerk And Play + Get Caught.avi”

19 This 58-minute video depicts two prepubescent males on a webcam sitting on
20 what appears to be a bed. Both males remove their clothing and proceed to
21 engage in both manual and oral sex. Based on lack of pubic hair, muscular
22 development, and youthful appearance, both males are approximately 9 years old
23 (as indicated by the file name).

24 C. Procedural History & Plea Agreement

25 Following thorough negotiation and consideration of the unique circumstances posed
26 by this case, the parties reached a pre-indictment plea agreement. On January 31, 2020,
27 Defendant Hernandez made his initial appearance in this District and entered guilty pleas to
28 counts of *Computer Fraud and Abuse*, in violation of Title 18, United States Code, Section

1030(a)(2), and *Possession of Child Pornography*, in violation of Title 18, United States Code, Section 2252(a)(4)(B), charged by Superseding Information (Dkt. #6).⁹

In the Plea Agreement (Dkt. #11), the parties entered into multiple stipulations. Most notably, the parties agreed to jointly recommend that the Court impose “a term of imprisonment of 36 months on each count, to run concurrently.” *Id.* at ¶ 14.

The parties also stipulated as to various sentencing factors, including the computation of Defendant Hernandez’s offense level computations under the U.S. Sentencing Guidelines for each offense of conviction. *Id.* at ¶¶ 12-13. These calculations are set forth in detail below, and included the defendant’s acknowledgement that his hacking conduct caused loss to his primary victim, Nintendo, of “more than \$3,500,000.” *Id.* at ¶ 12.

Defendant Hernandez agreed to forfeit and abandon any interest in the various electronic devices used to commit the hacking and child pornography offense. *Id.* at ¶¶ 9-10. Further, the defendant agreed to pay restitution to Nintendo in the amount of \$259,323.82. *Id.* at ¶ 8. He also agreed to register as a sex offender. *Id.* at 15.

The Plea Agreement also contained a limited waiver of appeal. *Id.* at ¶ 18. Assuming the Court imposes a term of incarceration that is within or below the Sentencing Guidelines range as determined by the Court at the time of sentencing, the United States requests that the Court advise Defendant appropriately regarding his remaining appellate rights, following imposition of sentence.

C. Conduct on Bond

Defendant Hernandez was released on an appearance bond with special conditions (Dkt. #13) allowed to return to his residence in Palmdale, California. The bond contained multiple prohibitions on use of electronic devices and the Internet, such as:

- “The defendant shall not use, possess or have access to a computer or computer components . . . at the defendant’s residence”;

⁹ An initial Information (Dkt. #1) was filed on December 18, 2019, in order for Hernandez’s counsel to submit an application for leave to appear pro hac vice, which was granted.

- 1 • “The defendant shall not use, possess, or have access to PDA’s, gaming
- 2 systems, and Internet enabled TV devices, nor access the internet through use
- 3 of a cellular phone device.”
- 4 • “The defendant shall not access the internet, or private or public computer
- 5 networks, or not have others do so on his/her behalf, without prior approval of
- 6 Pretrial Services.”

7 The bond also prohibited unauthorized contact with, and proximity to, minors, such as:

- 8 • “The defendant shall not go to places, enter, nor loiter in or around areas
- 9 where minors are known to congregate”;
- 10 • “You shall not have contact with any person under the age of 18 without the
- 11 permission of the Pretrial Service Office.”

12 On about November 9, 2020, Defendant Hernandez was arrested at his Palmdale,
 13 California residence on a warrant requested by the Pretrial Office and issued by this Court.
 14 The Pretrial Office alleged that Hernandez “violated the special condition requiring he not
 15 access the internet or have others do so on his behalf without prior approval of Pretrial
 16 Services by accessing the internet since on or before April 2020.” The defendant ultimately
 17 appeared in this District, by videoconference, on November 19, 2020, and admitted the
 18 violation. Dkt. #38.

19 As set forth in the violation report, in July 2020, the Pretrial Services officer first
 20 received information from a concerned third party that Defendant Hernandez remained
 21 active on social media and was using an “unmonitored” phone. The Pretrial Services Office
 22 in the Central District of California contacted Defendant Hernandez and his father who
 23 denied any internet use or device usage.

24 In September 2020, the Pretrial Services Office again received a complaint from a
 25 concerned third party that Defendant Hernandez remained active in online forums,
 26 including Discord, and was in contact with a minor, with whom he shared a YouTube
 27 channel. The reporting party provided links to the defendant’s posts.

1 This unapproved Internet access was confirmed through account activity records
 2 obtained from service providers. For example, according to login records from Discord,
 3 Hernandez accessed his Discord account on a daily basis, dating back to at least early April
 4 2020 through the present. Nearly every login occurred through the IP address
 5 (104.173.88.21) assigned to his Palmdale, California residence. An excerpt of the
 6 voluminous Discord logs and subscriber records from Charter Communications,
 7 Hernandez's home Internet Service Provider, are attached as **Exhibit 1** (under seal).

8 In other words, Hernandez possessed an unauthorized device and continued to access
 9 the Internet, from his home, for many months beginning shortly after being released on
 10 bond. Moreover, through such online forums, he almost certainly remained in contact with
 11 minors. Also significant, he also was not truthful with the pretrial officer who visited his
 12 residence and interviewed him in July 2020.

13 III. GUIDELINES CALCULATION

14 The government concurs with the Probation Office's application of the United States
 15 Sentencing Guidelines ("USSG"). In the Plea Agreement, the United States and Defendant
 16 Hernandez stipulated to the calculation of the advisory range, as set forth below.

17 Defendant Hernandez falls within criminal history category I, as he has no prior
 18 convictions. PSR ¶ 50.

19 Assuming that the Court finds that the defendant has sufficiently accepted
 20 responsibility at the time of sentencing, Defendant Hernandez's Total Offense Level (TOL)
 21 is 26. PSR ¶¶ 23-47. As set forth in the PSR and the parties' Plea Agreement, the
 22 following provisions apply:

23 **Count 1: Computer Fraud and Abuse (Hacking)**

- 24 1. a base offense level of 6, pursuant to USSG § 2B1.1.
- 25 2. an 18-level increase, pursuant to USSG § 2B1.1(b)(1)(J), because the offense
 26 involved a total loss amount of greater than \$3,500,000 but less than
 27 \$9,500,000.

3. a 2-level increase, pursuant to USSG § 2B1.1(b)(10), because the offense involved sophisticated means.

4. an Adjusted Offense Level for Count 1 of 26.

Count 2: Possession of Child Pornography

1. a base offense level of 18, pursuant to USSG. § 2G2.2.

2. a 2-level increase, pursuant to USSG § 2G2.2(b)(2), because Defendant Hernandez possessed illicit material involving prepubescent minors who had not attained the age of 12 years.

3. a 2-level increase, pursuant to USSG § 2G2.2(b)(6), because the offense involved the use of a computer or an interactive computer service.

4. a 5-level increase, pursuant to USSG § 2G2.2(b)(7)(D), because Defendant Hernandez possessed over 600 illicit images, more specifically, 669 images and 968 videos of minors engaged in sexually explicit conduct. (According to USSG §2G2.2 Application Note 6(B), each video equates to 75 images for guidelines purposes. Thus, Defendant Hernandez possessed 73,269 images of child pornography.)

5. an Adjusted Offense Level for Count 2 of 27.

Multiple Count Adjustment / Total Offense Level (TOL)

1. a total number of units of separately grouped counts of 2.

2. a Combined Adjusted Offense Level of 29.

3. a 3-level decrease, pursuant to USSG § 3E1.1, based on a sufficient acceptance of responsibility.¹⁰

4. a TOL of **26**.

Accordingly, as set forth in the presentence report, Defendant Hernandez's advisory range of imprisonment, based upon a criminal history category I and TOL 26, is **63 to 78 months**.

¹⁰ The United States moves for the discretionary 1-level decrease pursuant to USSG § 3E1.1.(b).

IV. RECOMMENDATION AND JUSTIFICATION

The government respectfully recommends terms of incarceration of **36 months** on both Count 1 and 2, to be served concurrently, to be followed by seven (7) years of supervised release, subject to the recommended standard and special conditions. The U.S. Probation Office joins in this recommendation, and the defense has agreed that a 36-month term is appropriate. The government submits that this sentence is warranted by, and sufficient but not greater than necessary in light of the United States Sentencing Guidelines (USSG) as well as the factors set forth in 18 U.S.C. § 3553(a) for the reasons set forth below.

A. 18 U.S.C. § 3553(a) Factors

As the Ninth Circuit and the Supreme Court have made clear, the sentencing guidelines are “the ‘starting point and the initial benchmark’ . . . and are to be kept in mind throughout the process.” *United States v. Carty*, 520 F.3d 984, 996 (9th Cir. 2008) (internal citations omitted). Title 18, United States Code, Section 3553(a), sets forth factors for the Court to consider alongside the advisory guideline range. The United States submits that the recommended sentence is appropriate particularly in light of “the nature and circumstances of the offense,” “the history and characteristics of the defendant,” and the need for the sentence “to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offense,” and “to afford adequate deterrence to criminal conduct.” 18 U.S.C. §§ 3553(a)(1), (a)(2)(A), and (a)(2)(B).

Here, the nature and circumstances of the offenses of conviction are serious. Hernandez’s relentless hacking activity occurred over the course of years and continued despite opportunities and his empty promises to cease. As noted above, Hernandez holds a bizarre infatuation with Nintendo and its products, and a similarly strange craving for attention from others for exposing and exploiting Nintendo data and information. In 2016, Hernandez jeopardized the integrity of Nintendo information by accessing and publicly leaking confidential and proprietary developer tools, which facilitated piracy and other harmful conduct. Nintendo, through its representatives, attempted to resolve the situation,

1 | securing Hernandez's and his parents' promises that such conduct would cease. Not so. In
2 | October 2016, just a month after the aforementioned promises, Hernandez participated in a
3 | significant hack of Nintendo's developer tool portal, making use of a designed phishing
4 | message and credential scraping malware. In October 2017, the FBI contacted Hernandez
5 | and again he and his parents promised that such conduct would stop and that he understood
6 | the consequences of hacking. Given Hernandez's age and role, the government exercised
7 | restraint, electing not to pursue criminal charges.

8 | That outcome had the opposite intended impact on Hernandez, as escaping
9 | consequences for very serious misconduct appears to have emboldened, rather than deter,
10 | him. Despite his promises, Hernandez continued to target and victimize Nintendo, also
11 | elevating the sophistication of his attacks. By at least mid-2018, Hernandez was hacking
12 | into Nintendo servers and exfiltrating data. He further used stolen credentials and
13 | certificates and knowledge gained from each hacked servers to exploit and access additional
14 | server groups, moving laterally through and expanding his footprint within Nintendo's
15 | network. He gained access to and downloaded an immense amount of data, largely
16 | targeting video games, consoles, and developer tools. Exacerbating the harm to the victim,
17 | Hernandez publicized his thefts and shared access to the stolen data to others in his
18 | community.

19 | Hernandez's tenacious conduct has measurable consequences to his intended victim,
20 | Nintendo. As acknowledged in the Plea Agreement, Hernandez's hacking conduct caused
21 | Nintendo multiple millions of dollar (over \$3.5 million) in damages and compelled
22 | Nintendo to expend hundreds of thousands of dollars in investigation and remediation
23 | efforts. Still, Hernandez's conduct has caused lasting harms that go beyond the direct
24 | financial impact. As set forth in Nintendo's victim impact statement, also before the Court:

25 | The first crime Mr. Hernandez committed against Nintendo was
26 | accomplished by impersonating a business partner needing support
27 | and then leveraging stolen login tokens. As a result, and as one
28 | example, Nintendo has implemented more arduous and cumbersome
 processes for partners to follow to get legitimate support. This

1 causes ongoing expense, and also makes it harder for the entire
2 industry to go about their day-to-day tasks.

3 Indeed, by exposing proprietary files and information, Hernandez effectively aided other
4 bad actors intent on harming Nintendo and its partners:

5 [T]he confidential information Mr. Hernandez published is useful to
6 other hackers interested in enabling the playing of pirated games on
7 Nintendo's game consoles. As a result, many game developers such
8 as Nintendo have lost revenue associated with those pirated games.
9 Mr. Hernandez was part of that piracy "scene" and so knew
precisely what the impact would be, releasing the content with this
end in mind.

10 In short, the substantial toll of direct and derivative harms, financial and
11 otherwise, caused by Hernandez's utter disregard for the law and the property
12 rights of others is an aggravating factor that the Court should consider in imposing
13 sentence.

14 Still more, Hernandez further exhibited no sign of stopping, but rather continued to
15 methodically work his way through Nintendo's networks in search of confidential files and
16 information. Only Nintendo's discovery of the unauthorized network access coupled with
17 the FBI's diligence identified Hernandez as the perpetrator and finally halted his intrusions,
18 at least for the time being.

19 The FBI's June 2019 search of his residence and seizure of his devices disrupted and
20 impeded his ability to hack. Even so, as exhibited by the recently discovered egregious
21 violations of his pretrial bond, Hernandez shows little willingness to abide by the rules,
22 even when presented with federal criminal charges. Past conduct being a fair indicator of
23 future behavior, the government submits that Hernandez presents a high risk of re-offense.

24 Separately, but equally troubling, Hernandez possessed (and received) thousands of
25 images (specifically, 669 graphics and 968 videos) of particularly disturbing child
26 pornography. As described above, the defendant's interests appear to focus on
27 prepubescent minors, engaging in explicit sexual acts with one another. Further, his method
28

1 of organizing and storing such files, within subfolders titled “cute,” “eh,” “okish,” etc.,
2 suggest that he rated such lascivious material based on his personal preferences and
3 fondness. Based on his history of hacking and his performance on pretrial release,
4 Hernandez has demonstrated little ability to regulate or control his proclivities.

5 The Court must also consider the history and characteristics of the defendant, and the
6 government acknowledges that this §3553(a) factor on balance weighs in favor of
7 mitigation. Despite all his mischief and run-ins with Nintendo, Hernandez remains only 21
8 years old and has no documented criminal history. By all accounts, he had a middle-class
9 upbringing with access to education and resources and remains surrounded by a supportive
10 family. Further, Hernandez has been diagnosed with a disorder, which is described in more
11 detail in the presentence report and the evaluation report submitted by Hernandez. These
12 unique circumstances were fully considered and weighed heavily into the negotiated pre-
13 indictment resolution reached between the parties, which contemplates a stipulated
14 recommendation below the advisory sentencing guidelines range.

15 The Bureau of Prisons (BOP) has been apprised of Hernandez’s claimed mental
16 health concerns and is fully prepared and equipped to address them during his term in
17 custody. As set forth in the Declaration of Tamara Klein, BOP Mental Health Treatment
18 Coordinator, attached as **Exhibit 2** (under seal), upon sentencing, defendants such as
19 Hernandez will be independently evaluated for mental conditions by trained professionals,
20 which includes (unlike the defense report) review of existing medical and psychological
21 records. Based on that assessment, BOP will designate a defendant appropriately. The
22 BOP currently operates specialized facilities and programs for inmates suffering from
23 certain disorders, including a SKILLS Program, a unit-based treatment program designed to
24 improve adjustment of inmates with intellectual and social impairments. As of February
25 2020, BOP successfully housed and managed approximately 70 similarly diagnosed
26 inmates. In sum, assuming the accuracy of Hernandez’s diagnosis, BOP is amply equipped
27 to successfully manage and treat his condition during a term of incarceration.
28

That said, while the government acknowledges that Hernandez may suffer from legitimate medical concerns, it nevertheless is compelled to highlight certain facts and share additional information that helps illuminate the seemingly modest severity of Hernandez's impairments. For example,

- Hernandez's diagnosis occurred in August 2019, *after* FBI's search of his residence in June 2019 and after the filing of federal charges became readily apparent. He was first evaluated in July 2019, specifically in anticipation of the filing charges. *See* Defense Report at pg. 1 ("Ryan's attorney recommended an assessment after Ryan was given legal charges for cyber crimes.").
- The evaluation acknowledges that Hernandez has an average IQ.
- The evaluation itself bears apparent flaws and shortcomings in its foundation. Evaluators were not provided with background records, source material, or substantial pertinent information, including, among other things, education records discussed herein or prior medical records. Rather, the evaluation and diagnosis were narrowly based on their interview and observations of Hernandez (and information provided by him and his parents) in July 2019.

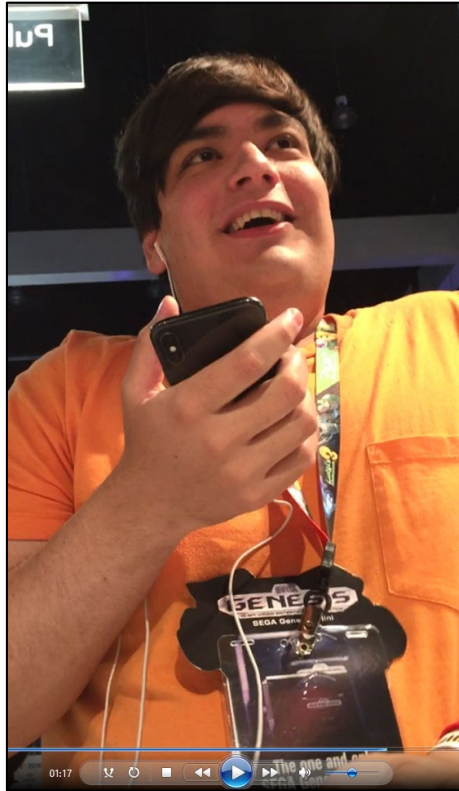
In many other interactions and scenarios (not provided to evaluators), Hernandez operated seemingly normally with others. For instance,

- For multiple years, including in 2019, Hernandez attended the Electronic Entertainment Expo, commonly known as "E3," a popular annual event for the video game industry, held in Los Angeles, California.¹¹ A primary purpose of E3 is for visitors to interact in-person with one another and representatives from the various video game and console developers. Attached as **Exhibit 3**,¹² is a two-minute-and-ten-second (2:10) video recording of Hernandez talking

¹¹ *See, e.g.*, <https://en.wikipedia.org/wiki/E3> (last visited 11/24/2020).

¹² A copy of the recording will be provided to the Court and the Clerk's Office on a compact disc. The recording previously has been provided to the U.S. Probation Office and counsel for Hernandez.

freely, extensively, and eloquently to a complete stranger (specifically, a representative working at a Nintendo kiosk) at the 2019 E3 event, held on June 11-13, 2019 --- *i.e.*, the week before the search of Hernandez's residence. A screenshot from the video follows:



It was later discovered that Hernandez also was recording the same conversation, which he posted or streamed through one of his many social media accounts. Further noteworthy is the substance of Hernandez's conversation. As captured in the recording, Hernandez repeatedly asked the Nintendo representative technical questions related to Nintendo server infrastructure and data protection measures (e.g., "lotcheck" and "white list"), which involved matters directly pertaining to his then-ongoing hacking efforts against the company.

- Similarly, a review of Hernandez's AT&T phone records and usage logs (number ending in -3779) confirms frequent voice calls. An excerpt of

voluminous call records, showing multiple thousands of individual voice calls prior to June 18, 2019 (the date of FBI's search of his residence), is attached as **Exhibit 4** (under seal).¹³

- Hernandez's educational records show little, if any, suggestion of impairments or the now-proffered diagnosis. For example, after graduating from high school, Hernandez attended Antelope Valley College from 2017 to 2019, relevant excerpts from which are attached as **Exhibit 5** (under seal). His college application records denote that he initially indicated a major of General Business and expressed interest in obtaining an associate degree before transferring to a 4-year institution. Also significant, when Hernandez registered for career services, he affirmatively noted "none" when asked what "obstacles or challenges are you currently facing?" In doing so, he specifically did *not* indicate any "Disability/Health issue" or any other possible impediment to his career development.

In short, while Hernandez may well have a medical condition, evidence shows that Hernandez appears to be functioning member of the society notwithstanding his recent diagnosis.

The government's recommendation further is driven by the seriousness of the offenses and the need to deter this defendant and others, to protect the public, and to impose just punishment. As discussed above, Hernandez committed a variety of offenses and has pled guilty to two distinct federal felony crimes. He has a history of demonstrated recalcitrance and unwillingness to abide by rules that suggests a meaningful punishment is necessary to protect the public and to deter him and similar defendants from engaging in similar conduct. As adeptly articulated by the victim itself,

The defendant was provided multiple, escalating warnings from

¹³ To be clear, Exhibit 4 reflects only voice usage, in which Hernandez necessarily communicated orally. By contrast, associated records of Hernandez's SMS (text) and data usage, which are likewise substantial, are not included. Because the records contain various phone numbers, including those of third parties, the government seeks to file this exhibit under seal.

1 Nintendo and Law Enforcement, making clear that the behavior he
2 was pursuing was illegal. Despite these warnings the defendant
3 continued to attack Nintendo and promote this type of activity
4 throughout the community, hosting discussion boards for aspiring
5 hackers, for example. Blatantly disregarding the warnings of victims
6 and law enforcement, and indeed flaunting that disregard, creates a
7 perception by others that this behavior is acceptable and shows that
8 Mr. Hernandez would likely return to his illegal activities if given
9 the chance.

10 When active, Hernandez served as a motivating influence for aspiring hackers, encouraging
11 and equipping others to engage in illegal activity by sharing his exploits as well as his loot.
12 Now being sentenced for his criminal endeavors, the circumstances call for a
13 correspondingly meaningful sentence that deters both Hernandez as well as aspiring hackers
14 from such harmful and self-destructive conduct.

15 That said, as noted, the United States recognizes factors that weigh in mitigation and
16 agrees that a sentence below the advisory guideline range is appropriate under the
17 circumstances. It is significant to recognize that the current recommendation, which
18 involves a total term of incarceration of 36 months, is the product of negotiation by the
19 parties in contemplation of the various and at times competing factors set forth in 18 U.S.C.
20 § 3553(a). The United States requests that this Court follow the parties' agreement and
21 impose such a custodial term as part of Hernandez's sentence.

22 In fashioning a sentence, the Court also must consider the "need to avoid
23 unwarranted sentence disparities" among "defendants with similar records who have been
24 found guilty of similar conduct." 18 U.S.C. § 3553(a)(6). In short, the government is
25 unaware of any defendant, anywhere, that is similarly situated to Defendant Hernandez. As
26 discussed above, he committed both hacking and child pornography offenses, and presents
27 unique characteristics that distinguish him from other defendants sentenced in this District
28 and elsewhere. Regardless, each case poses its own distinct circumstances and the
government offers this information merely to emphasize that the parties' recommendation is

1 consistent with disparity considerations.¹⁴

2 It is truly unfortunate that, after numerous warnings and opportunities to reflect upon
3 his misconduct, the defendant nevertheless returned to hacking activity. It is even more
4 unfortunate that with each opportunity Hernandez's conduct escalated in levels of severity
5 and brashness. The United States sincerely hopes that Defendant Hernandez finally learns
6 his lesson and abides by the laws prohibiting the victimization of others and the receipt and
7 possession of child pornography. A meaningful term of incarceration is warranted, to be
8 followed by an extended period of supervised release.

9 **B. Forfeiture**

10 As set forth in the Preliminary Motion for Entry of Preliminary Order of Forfeiture
11 (Dkt. #30) and the Plea Agreement (Dkt. #11), the following six (6) items are subject to
12 forfeiture:

- 13 1. One Seagate external hard drive, serial no. Z84112WS;
- 14 2. One Apple Macbook, serial no. C02MN8TDFD57;
- 15 3. Nintendo Switch console, serial no. XAW10001300634;
- 16 4. Nintendo Switch console, serial no. XAW10021377616;
- 17 5. IS-Nitro-Emulator, serial no. 08050639; and,
- 18 6. NDEV wireless device, serial no. NMA20089065.

19 On November 23, 2020, the Court enter the Preliminary Order. Dkt. #39.

20 **C. Restitution and Fines**

21 As part of the Plea Agreement, the defendant has agreed to pay restitution to
22 Nintendo in the amount of \$259,323.82. Dkt. #11 at ¶ 8. The United States requests that
23 that restitution order be included in the sentence and final judgment.

24
25
26
27
28 ¹⁴ Given that parties do not have access to the presentence report and other material information related to other cases, the government believes that sentence disparity offers only limited value across separate cases.

1 The United States concurs in the recommendation of the Probation Office that the
2 fine be waived based on the defendant's apparent inability to pay. However, the defendant
3 is responsible for the mandatory Special Assessment of \$200.

4 **V. CONCLUSION**

5 For the reasons set forth above, the United States respectfully recommends that the
6 Court sentence the defendant, Ryan Hernandez, to custodial terms of 36 months on Count 1
7 and 2, to be served concurrently, followed by seven (7) years of supervised release subject
8 to the conditions recommend by the U.S. Probation Office.

9 Dated this 25th day of November, 2020.

10 Respectfully submitted,

11 BRIAN T. MORAN
12 United States Attorney

13 /s/ Steven T. Masada
14 STEVEN T. MASADA
15 Assistant United States Attorney
16 United States Attorney's Office
17 700 Stewart Street, Suite 5220
18 Seattle, Washington 98101
19
20
21
22
23
24
25
26
27
28